Computers & Security, 13 (1994) 85

Author Index for Vol. 12

Abrams, M.D., 679
Agnew, G.B., 501
Allinson, C., 781
Amoroso, E.G., 679
Arnett, K.P., 191
Aßmann, R., 477

Badenhorst, K.P., 597
Banks, W.W., 51
Bergen, H.A., 157, 781
Beth, T., 753
Black, D.K., 437

Caelli, W., 640
Chen, N.-S., 191
Clyde, R.A., 123
Cohen, F.B., 275, 565
Collins, B.S., 629
Cumming, A., 136

Damm, F., 753
Davies, D., 32
Dawson, E., 781
Di Turi, B.B., 447
Donovan, S., 28
DuBois, D., 235

Eloff, J.H.P., 597

Fagan, P., 710
Fernández-González, J., 501
Fitch, J.A., 169
Ford, J., 235

Gollmann, D., 753
Graham, I., 640

Hardy, G., 716
Heinlein, E.B., 334, 435, 627
Highland, H.J., 4, 33, 106, 139, 216, 249, 259, 322, 362, 424, 456 518, 550, 612, 634, 698, 730
Hochberg, J., 235
Hoffman, L.J., 169
Hogan, J.M., 157

Jackson, K., 235
Jones, M.C., 191

Kensey, M.F., 536
Koerner, F., 775

Labuschagne, F., 469, 597
LaPadula, L.J., 679
Lathrop, D.L., 135
Lawrence, L.G., 15, 230
Longstaff, T.A., 61
Lunt, T.F., 405, 679

McClary, J.F., 235
Matthews, S., 629
Meyer, J., 338
Moseley, D., 128

Norman, G., 225

Obaidat, M.S., 657
O'Connor, L., 640
Ølnes, J., 765

Payne, J.E., 275
Pfitzmann, A., 477
Plant, M., 623
Pujals, J.M., 22

Rangan, P.V., 305
Reitenspiess, M., 341
Ribagorda, A., 501
Roberts, S., 137, 255
Roos, J., 469
Russell, S., 542

Saiedian, H., 79
Sandhu, R.S., 285
Schramm, C., 379
Schulz, E.E., 61
Slack, J.M., 389
Spafford, E.H., 585
Stahl, S.H., 117
Stallings, C., 235
Suri, G.S., 285

Tang, J.-T.E., 191

Unger, E.A., 79, 389

Vaughn, R.B., 79
Voas, J.M., 275,

Weeber, S.A., 585
Williams, J.G., 679
Wood, C.C., 51, 527, 663

0167-4048/94/$7.00 © 1994, Elsevier Science Ltd

Computers & Security, 13 (1994) 86-94

Subject Index for Vol.12

Access control
- a methodology for improving computer access security 657
- a view of information security tomorrow 634
- added-on security for MVS: weaknesses and measures 379
- cryptographic application programming interfaces (APIs) 640
- DECnet security (not necessarily an oxymoron) 123
- duress terminations and information security 527
- NADIR: an automated system for detecting network intrusion and misuse 235
- principles of secure information systems design with groupware examples 663
- public key management for X.25 network security 128
- report of an integrity research study group 679
- the role of roles 15

Accountability
- principles of secure information systems design with groupware examples 663

Accreditation
- commercial accreditation of information security 716

Adaptive model
- a chosen plaintext attack on an adaptive arithmetic coding compression algorithm 157

Anomaly detection
- NADIR: an automated system for detecting network intrusion and misuse 235

Application programming interfaces
- cryptographic application programming interfaces (APIs) 640

Arithmetic coding
- a chosen plaintext attack on an adaptive arithmetic coding compression algorithm 157

Assembly language,
- more efficient software implementations of (generalized) DES 477

Audit
- a survey of intrusion detection techniques 405
- getting management buy-in to IT security 623
- paradigms for verification of authorization at source of electronic documents in an integrated environment 542
- principles of secure information systems design with groupware examples 663

Authentication
- authentication services in distributed systems 753
- more efficient software implementations of (generalized) DES 477
- the authenticated datagram protocol: a high performance subtransport level secure communication protocol 305

Authorization
- paradigms for verification of authorization at source of electronic documents in an integrated environment 542

Authorship analysis
- software forensics: can we track code to its authors? 585

Automated risk analysis approaches
- a comparative framework for risk analysis methods 597

Automation
- NADIR: an automated system for detecting network intrusion and misuse 235

Availability
- recovery management 334

Block ciphers
- message collision in block ciphers with message authentication 781

0167-4048/94/$7.00 © 1994, Elsevier Science Ltd

Business
a view of information security tomorrow 634
perceptions of computer viruses: a cross-cultural assessment 191
securing your business process 629

Capabilities
a distributed capability-based architecture for the Transform model 285
Cascade problem
a shortest path network security model 169
Certificates
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
Channel efficiency
encryption and error correction codes for reliable file storage 501
Checksummers
computer viruses - towards better solutions 536
Chosen plaintext attack
a chosen plaintext attack on an adaptive arithmetic coding compression algorithm 157
CIPHER
security for EDIFACT messages 447
Clark-Wilson model
report of an integrity research study group 679
Classification techniques
a methodology for improving computer access security 657
Coding
encryption and error correction codes for reliable file storage 501
Communication
duress terminations and information security 527
Compatibility
securing your business process 629
Computational complexity
operating system protection through program evolution 565
Computer security. **Security**
Computer systems
a survey of intrusion detection techniques 405
a view of information security tomorrow 634
computer viruses - towards better solutions 536
digital signatures - explanation and usage 230
getting management buy-in to IT security 623
open system security standards 341
perceptions of computer viruses: a cross-cultural assessment 191
report of an integrity research study group 679
Computer viruses. **Viruses**
Confidentiality
duress terminations and information security 527
EDIFACT security made simple - the EDIMED approach 765
Contrary principle
system threats and vulnerabilities and the contrary principle 775
Corporate policy
organizational issues in IT security 710
Costs
principles of secure information systems design with groupware examples 663
securing your business process 629
Cryptography **Encryption**

Data compression
a chosen plaintext attack on an adaptive arithmetic coding compression algorithm 157
Data processing
NADIR: an automated system for detecting network intrusion and misuse 235
Data transmission
NADIR: an automated system for detecting network intrusion and misuse 235
Databases
duress terminations and information security 527
integrity in object-oriented database systems 389
NADIR: an automated system for detecting network intrusion and misuse 235
DECnet
beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code 61
DECnet security (not necessarily an oxymoron) 123

DES
EDIFACT security made simple - the EDIMED approach 765
more efficient software implementations of (generalized) DES 477
Design
human error: an overlooked but significant information security problem 51
principles of secure information systems design with groupware examples 663
Digital signatures
digital signatures - explanation and usage 230
the digital signature standard: overview and current status 437
Disaster recovery
disaster recovery after downsizing 225
Distributed systems
a distributed capability-based architecture for the Transform model 285
authentication services in distributed systems 753
information security in workstation environments 117
open system security standards 341
security of PCs in a distributed environment 28
Document identification
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
Domain constraints
integrity in object-oriented database systems 389
Dossiers
security and privacy 22
Downsizing
disaster recovery after downsizing 225
Duress terminations
duress terminations and information security 527

EDIFACT
EDIFACT security made simple - the EDIMED approach 765
security for EDIFACT messages 447
Electronic data interchange
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
securing your business process 629
security for EDIFACT messages 447
security of PCs in a distributed environment 28
Electronic documents
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
Electronic records
security and privacy 22
E-mail
security and privacy 22
Employment
duress terminations and information security 527
Encryption
a chosen plaintext attack on an adaptive arithmetic coding compression algorithm 157
authentication services in distributed systems 753
cryptographic application programming interfaces (APIs) 640
data security in X.25 networks 469
EDIFACT security made simple - the EDIMED approach 765
encryption and error correction codes for reliable file storage 501
more efficient software implementations of (generalized) DES 477
open system security standards 341
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
public key management for X.25 network security 128
the digital signature standard: overview and current status 437
Entrapment
principles of secure information systems design with groupware examples 663
Ergonomics
human error: an overlooked but significant information security problem 51

Error correction
encryption and error correction codes for reliable file storage 501
Error detection
NADIR: an automated system for detecting network intrusion and misuse 235
Errors and omissions
human error: an overlooked but significant information security problem 51
Expert systems
a survey of intrusion detection techniques 405
NADIR: an automated system for detecting network intrusion and misuse 235

False premise
system threats and vulnerabilities and the contrary principle 775
Fidelity insurance
duress terminations and information security 527
Forgery
digital signatures - explanation and usage 230
Fraud
digital signatures - explanation and usage 230
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
FUNACK
security for EDIFACT messages 447
Functional dependencies
integrity in object-oriented database systems 389

Globalization
securing your business process 629
Graph theory
a shortest path network security model 169
Graphical information systems
security and privacy 22
Groupware
principles of secure information systems design with groupware examples 663

IDES
a survey of intrusion detection techniques 405
Information Practices Act
security and privacy 22
Information security
a comparative framework for risk analysis methods 597
a view of information security tomorrow 634
commercial accreditation of information security 716
human error: an overlooked but significant information security problem 51
principles of secure information systems design with groupware examples 663
Information security responsibility
human error: an overlooked but significant information security problem 51
Information systems
report of an integrity research study group 679
securing your business process 629
Information technology
getting management buy-in to IT security 623
organizational issues in IT security 710
securing your business process 629
Integrated systems
NADIR: an automated system for detecting network intrusion and misuse 235
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
Integrity
a model for detecting the existence of software corruption in real time 275
EDIFACT security made simple - the EDIMED approach 765
report of an integrity research study group 679
Integrity protection
a model for detecting the existence of software corruption in real time 275
Inter-leaving
encryption and error correction codes for reliable file storage 501
Internet
open system security standards 341
Intrusion detection
a survey of intrusion detection techniques 405

NADIR: an automated system for detecting network intrusion and misuse 235
Inventory records
duress terminations and information security 527
Investigation
software forensics: can we track code to its authors? 585
ITSEC
commercial accreditation of information security 716

Kerberos
information security in workstation environments 117
open system security standards 341
Key management
data security in X.25 networks 469
EDIFACT security made simple - the EDIMED approach 765
integrity in object-oriented database systems 389

LAN systems
principles of secure information systems design with groupware examples 663
security of PCs in a distributed environment 28
Least privilege
principles of secure information systems design with groupware examples 663
Legal systems
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
Local modifications
added-on security for MVS: weaknesses and measures 379

Malicious code
beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code 61
software forensics: can we track code to its authors? 585
Management
duress terminations and information security 527
getting management buy-in to IT security 623
Man/machine interface
human error: an overlooked but significant information security problem 51
Message authentication
message collision in block ciphers with message authentication 781
Message collision
message collision in block ciphers with message authentication 781
Message unrecoverability
encryption and error correction codes for reliable file storage 501
Misuse detection
NADIR: an automated system for detecting network intrusion and misuse 235
Models
a model for detecting the existence of software corruption in real time 275
a survey of intrusion detection techniques 405
a survey of security issues in office computation and the application of secure computing models to office systems security models 79
report of an integrity research study group 679
Modes of operation
more efficient software implementations of (generalized) DES 477
Monitors
DECnet security (not necessarily an oxymoron) 123
Multiple data sources
NADIR: an automated system for detecting network intrusion and misuse 235
Multiple encryption
more efficient software implementations of (generalized) DES 477
Murphy's Law
I worked with Murphy 627
MVS
added-on security for MVS: weaknesses and measures 379

NADIR
NADIR: an automated system for detecting network intrusion and misuse 235

Network security
a shortest path network security model 169
Networks
data security in X.25 networks 469
DECnet security (not necessarily an oxymoron) 123
information security in workstation environments 117
NADIR: an automated system for detecting network intrusion and misuse 235
open system security standards 341
public key management for X.25 network security 128
security of PCs in a distributed environment 28
the authenticated datagram protocol: a high performance subtransport level secure communication protocol 305
Neural networks
a survey of intrusion detection techniques 405
Non-repudiation
EDIFACT security made simple - the EDIMED approach 765

Object-oriented databases
integrity in object-oriented database systems 389
Office information systems
a survey of security issues in office computation and the application of secure computing models to office systems 79
Open systems
open system security standards 341
Operating systems
open system security standards 341
operating system protection through program evolution 565

Parameterization
principles of secure information systems design with groupware examples 663

Passwords
a methodology for improving computer access security 657
a view of information security tomorrow 634
Pattern recognition
a methodology for improving computer access security 657
Peer-entity authentication
EDIFACT security made simple - the EDIMED approach 765
Personal computers
computer viruses - towards better solutions 536
duress terminations and information security 527
security of PCs in a distributed environment 28
Privacy
a survey of intrusion detection techniques 405
a survey of security issues in office computation and the application of secure computing models to office systems 79
information security in workstation environments 117
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
security and privacy 22
Program evolution
operating system protection through program evolution 565
Protection
a model for detecting the existence of software corruption in real time 275
a survey of security issues in office computation and the application of secure computing models to office systems 79
operating system protection through program evolution 565
report of an integrity research study group 679
Public key
authentication services in distributed systems 753
digital signatures - explanation and usage 230
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
public key management for X.25 network security 128
the digital signature standard: overview and current status 437
Public Records Act
security and privacy 22

RACF
added-on security for MVS: weaknesses and measures 379
Recovery management
disaster recovery after downsizing 225
recovery management 334
Redundancy
encryption and error correction codes for reliable file storage 501
Reference relationship
integrity in object-oriented database systems 389
Relationship constraints
integrity in object-oriented database systems 389
Remote services
DECnet security (not necessarily an oxymoron) 123
Reverse engineering
software forensics: can we track code to its authors? 585
Risk management
a comparative framework for risk analysis methods 597
a shortest path network security model 169
a view of information security tomorrow 634
getting management buy-in to IT security 623
human error: an overlooked but significant information security problem 51
I worked with Murphy 627
security and privacy 22
Roles
the role of roles 15
ROOT
the role of roles 15
RSA
public key management for X.25 network security 128

Safety
a distributed capability-based architecture for the Transform model 285
Security
a distributed capability-based architecture for the Transform model 285
a methodology for improving computer access security 657
a survey of intrusion detection techniques 405
a survey of security issues in office computation and the application of secure computing models to office systems 79
a view of information security tomorrow 634
added-on security for MVS: weaknesses and measures 379
commercial accreditation of information security 716
data security in X.25 networks 469
DECnet security (not necessarily an oxymoron) 123
duress terminations and information security 527
getting management buy-in to IT security 623
information security in workstation environments 117
NADIR: an automated system for detecting network intrusion and misuse 235
open system security standards 341
organizational issues in IT security 710
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
principles of secure information systems design with groupware examples 663
public key management for X.25 network security 128
report of an integrity research study group 679
securing your business process 629
security and privacy 22
security for EDIFACT messages 447
security of PCs in a distributed environment 28
the role of roles 15
Separation
system threats and vulnerabilities and the contrary principle 775
Shortest path
a shortest path network security model 169

Signatures
digital signatures - explanation and usage 230

the digital signature standard: overview and current status 437
Smartcards
information security in workstation environments 117
the digital signature standard: overview and current status 437
Software
added-on security for MVS: weaknesses and measures 379
computer viruses - towards better solutions 536
more efficient software implementations of (generalized) DES 477
software forensics: can we track code to its authors? 585
Software implementation of Data Encryption Standard
more efficient software implementations of (generalized) DES 477
Standards
more efficient software implementations of (generalized) DES 477
open system security standards 341
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
the digital signature standard: overview and current status 437
State integrity
integrity in object-oriented database systems 389
Statistical analysis
human error: an overlooked but significant information security problem 51
Subtransport protocol layer
the authenticated datagram protocol: a high performance subtransport level secure communication protocol 305
Synchronization
authentication services in distributed systems 753
System architectures
open system security standards 341

Systems management
NADIR: an automated system for detecting network intrusion and misuse 235

Threats
system threats and vulnerabilities and the contrary principle 775
Training
recovery management 334
Trusted systems
operating system protection through program evolution 565

Unix
the role of roles 15
User education
NADIR: an automated system for detecting network intrusion and misuse 235
User identification
public key management for X.25 network security 128
User privileges
duress terminations and information security 527

Validation
digital signatures - explanation and usage 230
Verification
paradigms for verification of authorization at source of electronic documents in an integrated environment 542
Viruses
beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code 61
computer viruses - towards better solutions 536
perceptions of computer viruses: a cross-cultural assessment 191
VMS
beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code 61
Vulnerabilities
system threats and vulnerabilities and the contrary principle 775

Workstations
information security in workstation environments 117
open system security standards 341

Worm
beyond preliminary analysis of the WANK and OILZ worms: a case study of malicious code 61

X.25
data security in X.25 networks 469
public key management for X.25 network security 128
Xephon
disaster recovery after downsizing 225